

DOCUMENT RESUME**ED 175 675****SE 028 663**

AUTHOR Syer, Henry W., Ed.
TITLE Supplementary and Enrichment Series: Factors and Primes. SP-17.
INSTITUTION Stanford Univ., Calif. School Mathematics Study Group.
SPONS AGENCY National Science Foundation, Washington, D.C.
PUB DATE 65
NOTE 58p.; For related documents, see SE 028 648-675; Contains occasional light and broken type

EDRS PRICE MF01/PC03 Plus Postage.
DESCRIPTORS Curriculum: *Division: *Enrichment: *Instruction: Mathematics Education: *Number Concepts: *Prime Numbers: Secondary Education: *Secondary School Mathematics: Supplementary Reading Materials
IDENTIFIERS *School Mathematics Study Group

ABSTRACT

This is one in a series of SMSG supplementary and enrichment pamphlets for high school students. This series is designed to make material for the study of topics of special interest to students readily accessible in classroom quantity. Topics covered include primes, factors, divisibility, greatest common factor, least common multiple, Robinson's Results, and Proth's Theorem. (MF)

* Reproductions supplied by EDRS are the best that can be made *
* from the original document. *

**SCHOOL
MATHEMATICS
STUDY GROUP**

SP-17

**SUPPLEMENTARY and
ENRICHMENT SERIES**

FACTORS AND PRIMES

Edited by Henry W. Syer

DEPARTMENT OF HEALTH
EDUCATION & WELFARE
NATIONAL INSTITUTE OF
EDUCATION

PERMISSION TO REPRODUCE THIS
MATERIAL HAS BEEN GRANTED BY

SMSG

TO THE EDUCATIONAL RESOURCES
INFORMATION CENTER (ERIC)



Financial support for the School Mathematics Study Group has been provided by the National Science Foundation.

© 1965 by The Board of Trustees of the Leland Stanford Junior University
All rights reserved
Printed in the United States of America

PREFACE

Mathematics is such a vast and rapidly expanding field of study that there are inevitably many important and fascinating aspects of the subject which, though within the grasp of secondary school students, do not find a place in the curriculum simply because of a lack of time.

Many classes and individual students, however, may find time to pursue mathematical topics of special interest to them. This series of pamphlets, whose production is sponsored by the School Mathematics Study Group, is designed to make material for such study readily accessible in classroom quantity.

Some of the pamphlets deal with material found in the regular curriculum but in a more extensive or intensive manner or from a novel point of view. Others deal with topics not usually found at all in the standard curriculum. It is hoped that these pamphlets will find use in classrooms in at least two ways. Some of the pamphlets produced could be used to extend the work done by a class with a regular textbook but others could be used profitably when teachers want to experiment with a treatment of a topic different from the treatment in the regular text of the class. In all cases, the pamphlets are designed to promote the enjoyment of studying mathematics.

Prepared under the supervision of the Panel on Supplementary Publications of the School Mathematics Study Group:

Professor R. D. Anderson, Department of Mathematics, Louisiana State University, Baton Rouge 3, Louisiana

Mr. Ronald J. Clark, Chairman, St. Paul's School, Concord, New Hampshire 03301

Dr. W. Eugene Ferguson, Newton High School, Newtonville, Massachusetts 02160

Mr. Thomas J. Hill, Montclair State College, Upper Montclair, New Jersey

Mr. Karl S. Kalman, Room 711D, Office of the Supt. of Schools, Parkway at 11st, Philadelphia 36, Pennsylvania 19103

Professor Augusta Schurrer, Department of Mathematics, State College of Iowa, Cedar Falls, Iowa

Dr. Henry W. Syer, Kent School, Kent, Connecticut

Professor Frank L. Wolf, Carleton College, Northfield, Minnesota 55057

Professor John E. Yarnelle, Department of Mathematics, Hanover College, Hanover, Indiana

FOREWORD

Without assuming any previous knowledge of the subject, this booklet discusses the following topics from simple number theory: basic definition, diagrams for factors, divisibility tests, casting out nines, complete factorization, greatest common factor, remainders in division, lowest common multiple, and some recent results by Robinson and Proth. The level of the treatment will make it useful in both junior and senior high schools. A separate teachers commentary with answers is available.

As background the reader will need little more than the arithmetic of positive whole numbers. However, the range of difficulty in this booklet is greater than in some: the beginning sections are very easy and the closing sections are rather difficult to read. This is done intentionally so that each reader can carry the ideas as far as he needs to. Our advice thus is: start at the beginning and read and work along as far as your interest and background allow you to do. You will profit from all you undertake and understand.

This material was originally published as part of the Junior High School texts and the Supplementary Units of SMSG.

CONTENTS

Section	Page
1. Primes	1
2. Factors	5
3. Diagram for Factors	10
4. Divisibility by 3 and 9	13
5. Casting Out the Nines	14
6. Why Does Casting Out the Nines Work?	17
7. Divisibility by 11	22
8. Divisibility by 7	23
9. Complete Factorization	26
10. Greatest Common Factor	28
11. Remainder in Division	32
12. Least Common Multiple	37
13. Sub-sets of Whole Numbers	41
14. Robinson's Results	45
15. Proth's Theorem	47

FACTORS AND PRIMES

1. Primes

We will assume that you are acquainted with two important sets of numbers: the counting numbers and the whole numbers.

Counting numbers: 1, 2, 3, 4, . . .

Whole numbers: 0, 1, 2, 3, . . .

It is also assumed that you know the arithmetic of these numbers; for example, how to add, subtract, multiply, and divide with them.

In this pamphlet we are interested in how counting numbers can be expressed as products of other counting numbers. For instance,

$$6 = 2 \times 3 = 1 \times 2 \times 3 = 1 \times 3 \times 2 = 1 \times 6 = 6 \times 1.$$

$$5 = 1 \times 5 = 5 \times 1 = 5 \times 1 \times 1.$$

$$12 = 2 \times 2 \times 3 = 4 \times 3 = 1 \times 2 \times 6 = 1 \times 3 \times 4.$$

Are there other ways in which these numbers can be expressed as products of counting numbers? Express the following as products of counting numbers in various ways: 15, 18, 30.

In the products listed above which are equal to 6, we see that 1, 2, 3, and 6 divide exactly into 6. That is, if 6 is divided by any one of these four numbers, the remainder is zero. Similarly, 1 and 5 are the only counting numbers that divide exactly into 5; while 1, 2, 3, 4, 6, and 12 are those which divide exactly into 12. Two other ways of making the same statement are:

1) The number 6 is divisible by 1, 2, 3, and 6.

2) The number 6 is a multiple of 1, 2, 3, and 6.

Thus, 5 is divisible by 1 and 5, or 5 is a multiple of 1 and 5; also, 12 is divisible by 1, 2, 3, 4, 6, and 12, or 12 is a multiple of each of the numbers 1, 2, 3, 4, 6, and 12.

On the other hand, 12 is not divisible by 5 since if 12 is divided by 5 the remainder is 2. For a similar reason, 6 is not divisible by 4.

The number 1 is in a class by itself since every counting number is a multiple of 1; that is, every counting number is divisible by 1. It is not true that every counting number is divisible by 2 (3 is not); not every counting number is divisible by 3 (24 is not); not every counting number is divisible by 19/6 (5 is not).

Every counting number is a multiple of 1 as we have seen. What are the multiples of 2 which are greater than 2? Let us look at one way to answer this question systematically: First write down the numbers, for instance, from 1 to 30 inclusive. The first multiple of 2 greater than 2 is 4; cross out the 4 and every second number after that. To keep track, write a 2 below each number you have crossed out. The list will then look like the following:

1 2 3 ~~4~~₂ 5 ~~6~~₂ 7 ~~8~~₂ 9 ~~10~~₂ 11 ~~12~~₂
 13 ~~14~~₂ 15 ~~16~~₂ 17 ~~18~~₂ 19 ~~20~~₂ 21 ~~22~~₂ 23 ~~24~~₂
 25 ~~26~~₂ 27 ~~28~~₂ 29 ~~30~~₂

We neither cross out 2 nor write a 2 under it because that is the number whose multiples we are considering. The numbers above which are not crossed out are 1, 3, and the numbers less than 31 which are not multiples of 2.

Our second step would be to go through the same table and cross out the multiples of 3 which are greater than 3. Then the table would look like this:

1 2 3 ~~4~~₂ 5 ~~6~~_{2,3} 7 ~~8~~₂ ~~9~~₃ ~~10~~₂ 11 ~~12~~_{2,3}
 13 ~~14~~₂ ~~15~~₃ ~~16~~₂ 17 ~~18~~_{2,3} 19 ~~20~~₂ ~~21~~₃ ~~22~~₂ 23 ~~24~~_{2,3}
 25 ~~26~~₂ ~~27~~₃ ~~28~~₂ 29 ~~30~~_{2,3}

Here we have crossed out every third number beginning with 6, but we have not crossed out 3 since that is the number whose multiples we are finding. (Some of the multiples of 3 had already been crossed out since they were also multiples of 2.) Except for the numbers 2 and 3, none of the numbers remaining are multiples of either 2 or 3.

As a class exercise, write out the numbers from 1 to 100 inclusive. First, cross out all multiples of 2 and 3 except 2 and 3 as we did above. The number 4 and all multiples of 4 are already crossed out since any multiple of 4 is also a multiple of 2. The next number not crossed

out is 5. So, for the third step cross out every fifth number after 5 (that is, beginning with 10), and write a 5 below each number crossed out. For the fourth and fifth steps, similarly cross out multiples of 7 and of 11 which are greater than 7 or 11 respectively. Keep track of the multiples as indicated. Did you cross out any new numbers when you were considering multiples of 11? Would we cross out any new numbers if we considered multiples of 12? of 13?

From the way in which the table was constructed you see that every number crossed out is a multiple of a smaller number different from 1. These numbers are called composite numbers.

Definition: A composite number is a counting number which is divisible by a smaller counting number different from 1.

The table which you have constructed by crossing out numbers is called the "Sieve of Eratosthenes" for the first 100 numbers.* It is called a "sieve" because in it you have sifted out all the composite numbers less than 100. Notice that when we crossed out the multiples of 2 and 3 less than 31, the composite number 25 remained. However, the number 25 was eliminated when we crossed out multiples of 5 in the third step. Similarly, the number 49 was not crossed out in the Sieve of Eratosthenes until we crossed out multiples of 7.

Except for the number 1, the numbers of the Sieve of Eratosthenes which are not crossed out are called prime numbers.

Definition: A prime number is a counting number, other than 1, which is divisible only by itself and 1.

Since it eliminates the composite numbers, the Sieve of Eratosthenes is a good way of finding a list of all prime numbers up to a certain point. The composite numbers are sifted out. The prime numbers remain. Why are the remaining numbers prime numbers?

The number 1 is not included in the set of primes partly because it is divisible by itself only. We shall have another stronger reason for this later on.

* Eratosthenes (c. 230 B.C.) was a friend of Archimedes and librarian at the University of Alexandria. He was interested in geography and mathematics.

Exercises 1

1. (a) List the prime numbers less than 100.
(b) Now list the prime numbers less than 130 but greater than 100.
2. (a) How many prime numbers are less than 50?
(b) How many prime numbers are less than 100?
(c) How many prime numbers are less than 130?

Do problems 3, 4, and 5 first without using Eratosthenes' Sieve and then use it to check your results.

3. List all the multiples of 5 which are less than 61.
4. List the set of numbers less than 50 which are multiples of 7.
5. List the set of numbers which are less than 100 and are also multiples of both 3 and 5.
6. In the table below, the numbers along the top represent values of a and those down the left side represent values of b. In each case if a is divisible by b, write the values of $\frac{a}{b}$ in the a-column and b-row. If a is not divisible by b, write "no" in the a-column and b-row.

	a = 12	14	17	18	20	25	27
b = 1							
b = 2							
b = 3							
b = 4							
b = 5							
b = 6							
b = 7							

7. Express each of the following counting numbers as a product of two smaller counting numbers or indicate that it is impossible to do this.
(a) 12 (c) 31 (e) 8 (g) 35 (i) 39 (k) 6 (m) 82
(b) 36 (d) 7 (f) 11 (h) 5 (j) 42 (l) 41 (n) 95

8. (a) By what numbers is 24 divisible?
 (b) The number 24 is a multiple of what numbers?
 (c) Are the two sets of numbers you have found in (a) and (b) the same? Why or why not?
 9. Write 12 in all possible ways as a product of counting numbers greater than 1.
 10. List the pairs of prime numbers less than 100 which have a difference of 2. How many are these? Such pairs are called twin primes.
 11. Express each even number between 4 and 22 as a sum of two prime numbers. (An even number, recall, is one divisible by 2.) Most mathematicians believe that every even number greater than 2 is the sum of two prime numbers but no one has been able to prove it. This is called "Goldbach's conjecture".
 12. Are there three numbers that might be called prime triplets?
 13. (a) Locate the numbers from 1 to 50 along a number line.
 (b) Underline the numerals in every second position, starting with 1.
 (c) Circle the numerals for the prime numbers.
 (d) Did you need to circle any numeral that was not underlined?
 If so, write all such numerals.
 14. What is the intersection of the set of prime numbers and the set of odd numbers less than 30?
-

2. Factors.

The word "factor" is commonly used in mathematics. Though the term may be new to you, the idea is not. We know that $5 \times 2 = 10$. Instead of calling one of the numbers the multiplicand and the other one the multiplier, we give both of them the same name -- factor. Thus, 5 and 2 are factors of 10; 6 and 7 are factors of 42, since $6 \times 7 = 42$. Also, $42 = 2 \times 3 \times 7$; so 2, 3, and 7 are factors of 42.

Example 1: Write 12 as a product of factors.

$$\begin{aligned}
 12 &= 1 \times 12, \\
 \text{or } 12 &= 2 \times 6, \\
 \text{or } 12 &= 3 \times 4, \\
 \text{or } 12 &= 2 \times 2 \times 3 = 2^2 \times 3.
 \end{aligned}$$

When we say "the factors" we mean "all the factors" of a number. For example, the number 6 has four factors, 1, 2, 3, and 6. The number 1 and the number itself are always factors of a number.

Example 2: Find the set of factors of 20.

The set of factors of 20 is $\{1, 2, 4, 5, 10, 20\}$.

The idea of factors is associated with multiplication. In mathematical symbols we define factor the following way:

Definition. If a , b , and c are whole numbers and if $ac = b$, then the number a is called a factor of b . (Under these conditions c is also a factor of b .)

Using the terms of the first section, we say that 3 is a factor of 12 because 12 is divisible by 3. In the symbols of the definition, we see that the number a is a factor of b if b is divisible by a .

The number 1 has only one factor, itself. Each prime number has exactly two factors, itself and 1. A composite number has how many factors?

Consider the number 24. It can be written as 4×6 . Both 4 and 6 are composite numbers since they can be written as products of smaller counting numbers: $4 = 2 \times 2$ and $6 = 2 \times 3$. Thus

$$24 = 2 \times 2 \times 2 \times 3.$$

However, 2 and 3 are prime numbers since they cannot be expressed as products of smaller numbers. We cannot go any further in this process. We therefore say that $2 \times 2 \times 2 \times 3$ is a complete factorization of 24.

Definition: If a counting number is written as a product of prime numbers, this product is called a complete factorization of the given number.

Example 1: Find a complete factorization of 20.

$$20 = 4 \times 5 = 2 \times 2 \times 5 = 2^2 \times 5.$$

Here 4×5 is not a complete factorization of 20 since 4 is not a prime number, but $2 \times 2 \times 5$ and $2^2 \times 5$ are complete factorizations. The most compact complete factorization of 20 is $2^2 \times 5$.

Example 2: Find a complete factorization of 72.

Method I

$$72 = 8 \times 9$$

$$72 = (4 \times 2) \times (3 \times 3)$$

$$72 = (2 \times 2) \times 2 \times (3 \times 3)$$

$$72 = (2 \times 2 \times 2) \times (3 \times 3)$$

Method II

Using continuing division

2	72
2	36
2	18
3	9
	3

Using exponents,

$$72 = 2^3 \times 3^2$$

$$72 = 2^3 \times 3^2$$

We might have used fewer steps. Notice that in both examples, the only factors appearing in the last products are prime numbers. Not all the factors of 20 and 72 (such as 4) appear in the final complete factorization. It is convenient but not necessary to use exponents wherever possible.

Note that $2 \times 5 \times 2$ is also a complete factorization of 20, but this is the same as $2 \times 2 \times 5$ except for the order of the factors. Similarly, in the factorization of 72, $2^2 \times 3 \times 2$ is the same as $2^3 \times 3$ except for the order of the factors. In fact, a very fundamental property of the counting numbers is that there is only one way to write a complete factorization of any counting number except for the order in which the prime factors appear. This property is given a special name:

The Unique Factorization Property of the Counting Numbers:

Every counting number greater than 1 can be factored into primes in only one way except for the order in which the factors occur in the product.

The word "unique" means that there is only one factorization except for order. (The question of order is another matter.) One might say that the Empire State Building is unique because there is no other building like it.

Here we have another reason for excluding 1 from the set of prime numbers. If we had called 1 a prime, then 5 could have been expressed as a product of primes in many different ways: 5×1 , $5 \times 1 \times 1$, $5 \times 1 \times 1 \times 1$, ... Here the product would not be unique except for the order in which the factors are written.

Exercises 2

1. List the set of factors for each of the following:

- | | | | |
|--------|--------|--------|--------|
| (a) 10 | (c) 9 | (e) 27 | (g) 11 |
| (b) 15 | (d) 18 | (f) 24 | |

2. Factor the numbers listed in as many ways as possible using only two factors each time. Because of the commutative property, we shall say that $3 \cdot 5$ is not different from $5 \cdot 3$.

- | | |
|---------|--------|
| (a) 10 | (e) 24 |
| (b) 15 | (f) 16 |
| (c) 9 | (g) 72 |
| (d) 100 | (h) 81 |

3. Write a complete factorization of:

- | | | | |
|--------|--------|--------|--------|
| (a) 10 | (c) 9 | (e) 45 | (g) 13 |
| (b) 15 | (d) 30 | (f) 50 | |

4. According to our definition of factor, is zero a factor of 6
Is 6 a factor of zero? Explain your answers.

5. (a) What factors of 20 do not appear in a complete factorization of 20?
(b) What factors of 72 do not appear in a complete factorization of 72?

6. Find a complete factorization of:

- | | |
|---------|----------|
| (a) 105 | (f) 345 |
| (b) 42 | (g) 311 |
| (c) 75 | (h) 1000 |
| (d) 500 | (i) 301 |
| (e) 64 | (j) 323 |

Definition. If a whole number is divisible by two it is an even number.
If a whole number is not divisible by two it is an odd number.

7. Tell whether these numbers are odd or even:

- | | |
|---------------------------|---------------------------|
| (a) 2×5 | (f) $3 \times 2 \times 6$ |
| (b) $3 + 7$ | (g) $128 - 37$ |
| (c) $6 \times 5 \times 3$ | (h) $3 \times 3 \times 7$ |
| (d) $2 + 16$ | (i) $3 \cdot (4 + 7)$ |
| (e) $7 + 8$ | (j) $5 \cdot (9 + 13)$ |

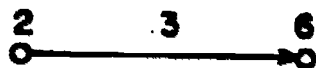
8. Copy the following table for counting numbers N and complete it through $N = 30$.

N	Factors of N	Number of Factors	Sum of Factors
1	1	1	1
2	1, 2	2	3
3	1, 3	2	4
4	1, 2, 4	3	7
5	1, 5	2	6
6	1, 2, 3, 6	4	12
7	1, 7	2	8
8	1, 2, 4, 8	4	15

- Which numbers represented by N in the table above have exactly two factors?
- Which numbers N have exactly three factors?
- If $N = p^2$ (where p is a prime number), how many factors does N have?
- If $N = pg$ (where p and g are different prime numbers), how many factors does N have? What is the sum of its factors?
- If $N = 2^k$ (where k is a counting number), how many factors does N have?
- If $N = 3^k$ (where k is a counting number), how many factors does N have?
- If $N = p^k$ (where p is a prime number and k is a counting number), how many factors does N have?
- Which numbers have $2N$ for the sum of their factors? These numbers are called perfect numbers. It is unknown how many perfect numbers there are or whether there are any odd perfect numbers.

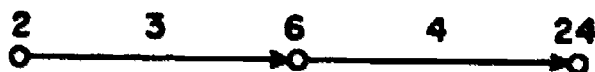
3. Diagrams for Factors

Basically, we can represent a product by the diagram



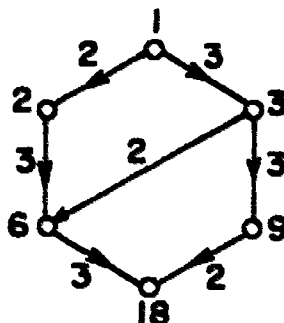
where the 3 associated with the line is the multiplier, which "takes 2 into 6". The arrow indicates the direction in which the multiplication goes.

Similarly



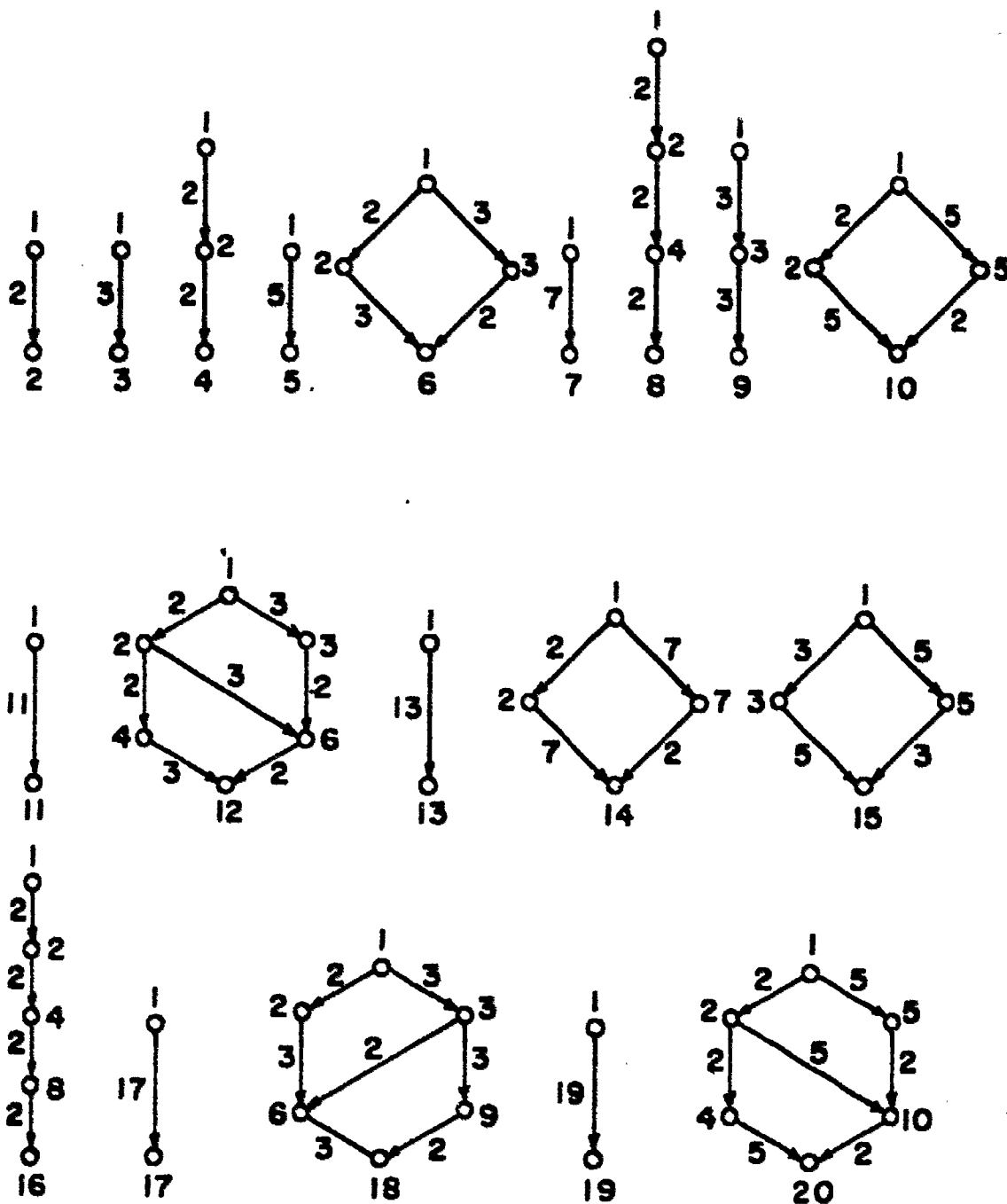
represents the product $(2 \times 3) \times 4$.

Then the three different complete factorizations of 18 could be represented by the following diagram. Notice that all the factors of 18 also appear in the diagram.



In making a diagram you may wish first to make a list of all the factors of the number and to arrange them from the smallest to the largest. For 12 this would be 1, 2, 3, 4, 6, 12. Then start with 1 and continue to build a chain so that the second number is divisible by the preceding number, and so on. Thus, one chain would consist of 1, 2, 4, and 12; another chain would consist of 1, 3, 6, and 12; and the last chain would be 1, 2, 6, and 12. In each of these chains, taking any pair, the second is divisible by the first and there is no factor between them. We could not go from 1 to 4 since there is the factor 2 between 1 and 4. Remember that one of the rules of the game is that there may be no other factor between successive numbers.

The diagrams for the numbers from 1 through 20 are shown here:

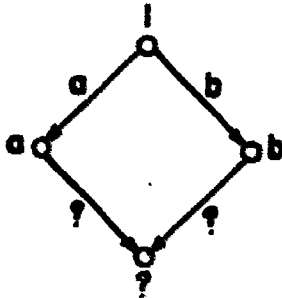


Some of you may be interested in pursuing the investigation of these diagrams a little further. The following examples are included for this purpose.

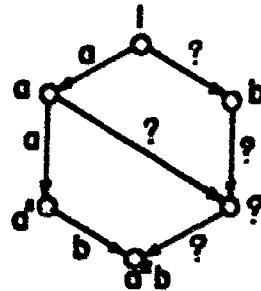
Exercises 3

1. Let a and b represent two different prime numbers. Complete each of the following sketches.

(a)



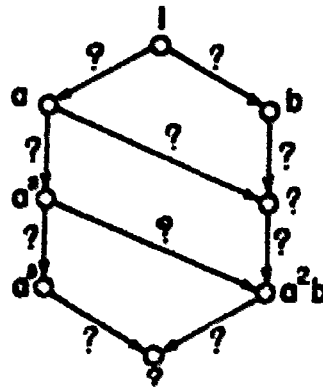
(c)



(b)



(d)



2. We have found that 6 and 10 had patterns like the one in Problem 1a. Name three other numbers that we have not sketched which have the same pattern.
3. Notice that 4 and 9 have the same pattern as Problem 1b. Name three others which we have not sketched that have the same pattern.
4. A number like 12 or 18 has the same pattern as Problem 1c. Find three other numbers which have this pattern.
5. Find three numbers which have patterns like Problem 1d.
6. Find patterns which have not been represented so far in the section.

4. Divisibility by 3 and 9

To find the factors of a number, we can always guess and try, but it is much easier if we can tell from looking at a number whether or not it has a given factor. From the Sieve of Eratosthenes it is clear that a number written in the decimal system is even if the last digit is even. As far as the sieve we have constructed goes, this is true. Thus:

A counting number written in the decimal system is even if its last digit is one of 0, 2, 4, 6, 8. If its last digit is not one of these, it is odd.

Suppose we see why this is so. To do this, remember how we found the multiples of 2 when we began to construct the Sieve of Eratosthenes. We started with the number and added 2 again and again. The last digits repeated in the pattern: 2, 4, 6, 8, 0, 2, 4, 6, 8, 0, ... This would continue no matter how far we extended the table. This shows that the even numbers are those whose last digit is one of the five numbers: 2, 4, 6, 8, 0.

In Problem 4 below you are asked to start with 5 and add 5 again and again to show the following:

A counting number expressed in the decimal system is divisible by 2 if its last digit is 0 or 5. Otherwise it is not divisible by 2.

What about divisibility by 3? Can we tell by looking at the last digit? The first ten multiples of 3 are

0, 3, 6, 9, 12, 15, 18, 21, 24, 27.

Each of the possible last digits, 0, 1, 2, 3, 4, 5, 6, 7, 8, and 9, appears in this list. On the other hand, none of the following are divisible by 3 even though each of the possible last digits appears here also:

4, 7, 10, 13, 16, 19, 22, 25, 28, 31.

We can see, then, that we cannot tell whether a number is divisible by 3 by looking at the last digit.

But suppose we add the digits of the multiples of 3. For 12 we have $1 + 2 = 3$; for 15 we have $1 + 5 = 6$; for 18 we have $1 + 8 = 9$. By this means we can form the following table:

Multiple of 3	0	3	6	9	12	15	18	21	24	27	30	33	36
Sum of digits	0	3	6	9	3	6	9	3	6	9	3	6	9

Multiple of 3	39	42	45	48	51	54	57	60	63	66	69	72
Sum of digits	12	6	9	12	6	9	12	6	9	12	15	9

Can you make any statement that seems to be true about the sum of the digits for all multiples of 3? You will see that in each case the sum of the digits is divisible by 3. Furthermore, if you add the digits of any number that is not divisible by 3 (take 25 where the sum of the digits is 7), the sum of the digits is not divisible by 3. Can you see why this will be true for all numbers? See Problem 3 in the next set.

You may notice that every third sum of digits in the table above is divisible by 9 and every third multiple of 3 is divisible by 9. Hence, we have the following test for divisibility by 9:

A number is divisible by 9 if the sum of its digits is divisible by 9. Otherwise, it is not divisible by 9.

5. Casting Out the Nines

You now know a very simple and interesting way to tell whether a number is divisible by 9. It is based on the fact that a number is divisible by 9 if the sum of its digits is divisible by 9; also, the sum of the digits of a number is divisible by 9 if the number is divisible by 9. For instance, consider the number 156782. The sum of its digits is $1 + 5 + 6 + 7 + 8 + 2$ which is 29. But 29 is not divisible by 9 and, hence, the number 156782 is not divisible by 9. If the second digit had been 2 less, the number would have been divisible by 9 since the sum of the digits would have been 27, which is divisible by 9. The test is a good one because it is easier to add the digits than to divide by 9. Actually we could have been lazy and, instead of dividing 29 by 9, use the fact again, add 2 and 9 to get 11, add the 1 and 1 to get 2 and see that since 2 is not divisible by 9, then the original six-digit number is not divisible by 9.

Why is this true? Merely dividing the given number by 9 would have tested the result, but from that we would have no idea why it would hold for any other number. We can show what is happening by writing out the number 156,782 in the decimal notation:

$$1 \times 10^5 + 5 \times 10^4 + 6 \times 10^3 + 7 \times 10^2 + 8 \times 10 + 2 =$$

$$1 \times (99999 + 1) + 5 \times (9999 + 1) + 6 \times (999 + 1) + 7 \times (99 + 1) + 8 \times (9 + 1) + 2.$$

Now, by the distributive property, $5 \times (9999 + 1) = (5 \times 9999) + (5 \times 1)$ and, similarly, for the other expressions. Also, we may rearrange the numbers in the sum since addition is commutative and associative. So, our number 156,782 may be written

$$1 \times (99999) + 5 \times (9999) + 6 \times (999) + 7 \times (99) + 8 \times 9 + (1 + 5 + 6 + 7 + 8 + 2).$$

Now 99999, 9999, 999, 99, 9 are all divisible by 9, the products involving these numbers are divisible by 9, and the sum of these products is divisible by 9. Hence, the original number will be divisible by 9 if $(1 + 5 + 6 + 7 + 8 + 2)$ is divisible by 9. This sum is the sum of the digits of the given number. Writing it out this way shows that no matter what the given number is, the same principle holds.

Exercises 2

1. (a) Test each of the numbers, 226843, 67945, 427536, and 45654 by the above method for divisibility by 9.
- (b) For any numbers in part (a) that are not divisible by 9, compare the remainders when the number is divided by 9 and when the sum of the digits is divided by 9.
- (c) From part (b) try to formulate a general fact that you suspect is true. Test this statement with a few more examples.

2. Choose two numbers. First, add them, divide by 9 and take the remainder. Second, divide each number by 9 and find the sum of the remainders; divide the sum by 9 and take the remainder. The final remainders in the two cases are the same. For instance, let the numbers be 69 and 79. First, their sum is 148, and the remainder when 148 is divided by 9 is 4. Second, the remainder when 69 is divided by 9 is 6, and when 79 is divided by 9 is 7; the sum of 6 and 7 is 13, and if 13 is divided by 9, the remainder is 4. The result is 4 in both cases. Why are the two results the same no matter what numbers are used instead of 69 and 79? Would a similar result hold for a sum of three numbers? (Hint: write 69 as $7 \times 9 + 6$.)
3. If in the previous exercise we divided by 7 instead of 9, would the remainders by the two methods for division by 7 be the same? Why or why not?
- * 4. Suppose in Exercise 2 we considered the product of two numbers instead of their sum. Would the corresponding result hold? That is, would the remainder when the product of 69 and 79 is divided by 9 be the same as when the product of their remainders is divided by 9? Would this be true in general? Could they be divided by 23 instead of 9 to give a similar result? Could similar statements be made about products of more than two numbers?
- * 5. Use the result of the previous exercise to show that 10^{20} has a remainder of 1 when divided by 9. What would its remainder be when it is divided by 3? by 99?
- * 6. What is the remainder when 7^{20} is divided by 6?
- * 7. You know that when a number is written in the decimal notation, it is divisible by 2 if its last digit is divisible by 2, and divisible by 5 if its last digit is 0 or 5. Can you devise a similar test for divisibility by 4, 8, or 25?
- * 8. In the following statement, fill in both blanks with the same number so that the statement is true.
 A number written in the system to the base 12 is divisible by _____ if its last digit is divisible by _____. If there is more than one answer, give the others, too. If the base were 7 instead of 12, how could the blanks be filled in? (Hint: One answer for base 12 is 6.)

* means these exercises are more difficult.

- *9. One could have something like "decimal" equivalents of numbers in numeration systems to bases other than 10. For instance, in the numeration system to the base 7, the septimal equivalent of $5(\frac{1}{7}) + 6(\frac{1}{7})^2$ would be written $.56_7$ just as the decimal equivalent of $5(\frac{1}{10}) + 6(\frac{1}{10})^2$ would be written $.56_{10}$ in the decimal system. The number $.142857142857 \dots$ is equal to $\frac{1}{7}$ in the decimal system, and in the system to the base 7 would be written $.1_7$. On the other hand, $.1_{10} = (.04620462 \dots)_7$. What numbers would have terminating septimals in the numeration system to the base 7? What would the septimal equivalent of $\frac{1}{5}$ be in the system to the base 7? (Hint: Remember that if the only prime factors of a number are 2 and 5, the decimal equivalent of its reciprocal terminates.)
- *10. Use the result of Exercise 3 to find the remainder when $9 + 16 + 23 + 30 + 37$ is divided by 7. Check your result by computing the sum and dividing by 7.
- *11. Use the results of the previous exercises to show that $10^{20} - 1$ is divisible by 9; $7^{108} - 1$ is divisible by 6.
- *12. Using the results of some of the previous exercises if you wish, shorten the method of showing that a number is divisible by 9 if the sum of its digits is divisible by 9.
- *13. Show why the remainder when the sum of the digits of a number is divided by 9 is the same as the remainder when the number is divided by 9.

6. Why Does Casting Out the Nines Work?

First, let us review some of the important results shown in the exercises which you did in Section 5. In Problem 2, you showed that to get the remainder of the sum of two numbers, after division by 9, you can divide the sum of their remainders by 9 and find its remainder. Perhaps you did it this way (there is more than one way to do it; yours may have been better). You know, in the first place, that any natural number may be divided by 9 to get a quotient and remainder. For instance, if the number is 725, the quotient is 80 and the remainder is 5. Furthermore, $725 = (80 \times 9) + 5$, and you could see from the way this is written that 5 is the remainder.

Thus, using the numbers in the exercise, you would write $69 = 7 \times 9 + 6$ and $79 = 8 \times 9 + 7$. Then $69 + 79 = (7 \times 9) + 6 + (8 \times 9) + 7$. Since the sum of two numbers is commutative and associative, you may reorder the terms and have $69 + 79 = (7 \times 9) + (8 \times 9) + 6 + 7$. Then, by the distributive property, $69 + 79 = [(7 + 8) \times 9] + 6 + 7$. Now, the remainder when $6 + 7$ is divided by 9 is 4, and $6 + 7$ can be written $(1 \times 9) + 4$. Thus, $69 + 79 = [(7 + 8 + 1) \times 9] + 4$. So, from the form it is written in, we see that 4 is the remainder when the sum is divided by 9. It is also the remainder when the sum of the remainders, $6 + 7$, is divided by 9.

Writing it out in this fashion is more work than making the computations the short way but it does show what is going on and why similar results would hold if 69 and 79 were replaced by any other numbers, and, in fact, we could replace 9 by any other number as well. One way to do this is to use letters in place of the numbers. This has two advantages. In the first place it helps us be sure that we did not make use of the special properties of the numbers we had without meaning to do so. Secondly, we can, after doing it for letters, see that we may replace the letters by any numbers. So, in place of 69 we write the letter a, and in place of 79, the letter b. When we divide the number a by 9 we would have a quotient and a remainder. We can call the quotient q and the remainder r . Then we have

$$a = (q \times 9) + r$$

where r is some whole number less than 9. We could do the same for the number b, but we should not let q be the quotient, since it might be different from the quotient when a is divided by 9. We here could call the quotient q' and the remainder r' . Then we would have

$$b = (q' \times 9) + r'.$$

Then the sum of a and b will be

$$a + b = (q \times 9) + r + (q' \times 9) + r'.$$

We can use the commutative and associative properties of addition to have

$$a + b = (q \times 9) + (q' \times 9) + r + r'$$

and the distributive property to have

$$a + b = [(q + q') \times 9] + r + r'.$$

Then, if $r + r'$ were divided by 9, we would have a quotient which we might call q'' and a remainder r'' . Then $r + r' = (q'' \times 9) + r''$ and

$$\begin{aligned} a + b &= [(q + q') \times 9] + (q'' \times 9) + r'' \\ &= [(q + q' + q'') \times 9] + r''. \end{aligned}$$

Now, r'' is a whole number less than 9 and, hence, it is not only the remainder when $r + r'$ is divided by 9 but also the remainder when $a + b$ is divided by 9. So, as far as the remainder goes, it does not matter whether you add the numbers or add the remainders and divide by 9.

The solution of Problem 4 goes the same way as that for Problem 2 except that we multiply the numbers. Then we would have

$$\begin{aligned} 69 \times 79 &= (7 \times 9 + 6) \times (8 \times 9 + 7) \\ &= [(7 \times 9) \times (8 \times 9 + 7)] + 6 \times (8 \times 9 + 7) \\ &= (7 \times 9 \times 8 \times 9) + (7 \times 9 \times 7) + (6 \times 8 \times 9) + (6 \times 7). \end{aligned}$$

The first three products are divisible by 9 and by what we showed in Problem 2; the remainder when 69×79 is divided by 9 is the same as the remainder when $0 + 0 + 0 + 6 \times 7$ is divided by 9. So, in finding the remainder when a product is divided by 9, it makes no difference whether we use the product or the product of the remainders.

If we were to write this out in letters as we did the sum, it would look like this:

$$\begin{aligned} a \times b &= (q \times 9 + r) \times (q' \times 9 + r') \\ &= (q \times 9 \times q' \times 9) + (q \times 9 \times r') + (r \times q' \times 9) + (r \times r'). \end{aligned}$$

Again, each of the first three products is divisible by 9 and hence the remainder when $a \times b$ is divided by 9 is the same as when $r \times r'$ is divided by 9.

We used the number 9 all the way above, but the same conclusions would follow just as easily for any number in place of 9, such as 7, 23, etc. We could have used a letter for 9 also, but this seems like carrying the generalization too far.

There is a shorter way of writing some of the things we had above. When letters are used, we usually omit the multiplication sign and write ab instead of $a \times b$ and $9q$ in place of $9 \times q$. Hence, the last equation above could be abbreviated to

$$ab = qq'9 \times 9 + qr'9 + rq'9 + rr'$$

or

$$ab = 9 \times 9qq' + 9qr' + 9rq' + rr'.$$

But this is not especially important right now.

So, let us summarize our results so far: The remainder when the sum of two numbers is divided by 9 (or any other number) is the same as the remainder when the sum of the remainders is divided by 9 (or some other number). The same procedure holds for the product in place of the sum.

These facts may be used to give quite a short proof of the important result stated in Problem 13 of Exercises 5. Consider again the number 156,782. This is written in the usual form:

$$(1 \times 10^5) + (5 \times 10^4) + (6 \times 10^3) + (7 \times 10^2) + (8 \times 10) + 2.$$

Now, from the result stated above for the product, the remainder when 10^2 is divided by 9 is the same as when the product of the remainders 1×1 is divided by 9, that is, the remainder is 1. Similarly, 10^3 has a remainder $1 \times 1 \times 1$ when divided by 9 and, hence, 1. So, all the powers of 10 have a remainder 1 when divided by 9. Thus, by the result stated above for the sum, the remainder when 156,782 is divided by 9 is the same as the remainder when $(1 \times 1) + (5 \times 1) + (6 \times 1) + (7 \times 1) + (8 \times 1) + 2$ is divided by 9. This last is just the sum of the digits. Writing it this way it is easy to see that this works for any number.

Now we can use the result of Problem 13 of Exercises 5 to describe a check called "casting out the nines" which is not used much in these days of computing machines, but which is still interesting. Consider the product 867×934 . We indicate the following calculations:

867 sum of digits: 21

sum of digits: 3

934 sum of digits: 16

sum of digits: 7

Product: 809,778

Product: $3 \times 7 = 21$

Sum of digits: $8 + 0 + 9 + 7 + 7 + 8 = 39$

Sum of digits: $3 + 9 = 12$

Sum of digits: $1 + 2 = 3$

Sum of digits: $2 + 1 = 3$.

Since the two results, 3, are the same, we have at least some check on the accuracy of the results.

Exercises 6

1. Try the method of checking for another product. Would it also work for a sum? If so, try it also.
2. Explain why this should come out as it does.
3. If a computation checks this way, show that it still could be wrong. That is, in the example given above, find an incorrect product that would still check.
4. Given the number $(5 \cdot 7^5) + (3 \cdot 7^4) + (2 \cdot 7^3) + (1 \cdot 7^2) + (4 \cdot 7) + 3$. What is its remainder when it is divided by 7? What is its remainder when it is divided by 6? by 3?
5. Can you find any short-cuts in the example above analogous to casting out the nines?
6. In a numeration system to the base 7, casting out what number would give a result corresponding to that in the decimal system when nines are cast out?
7. The following is a trick based on casting out the nines. Can you see how it works? You ask someone to pick a number -- it might be 1678. Then you ask him to form another number from the same digits in a different order -- he might take 6187. Then you ask him to subtract the smaller from the larger and give you the sum of all but one of the digits in the result. (He would have 4509 and might add the last three to give you 14.) All of this would be done without your seeing any of the figuring. Then you would tell him that the other digit in the result is 4. Does this trick always work?

One method of shortening the computation for a test by casting out the nines is to discard any partial sums which are 9 or a multiple of 9. For instance, if a product were 810,645, we would not need to add all the digits. We could notice that $8 + 1 = 9$ and $4 + 5 = 9$ and hence the remainder when the sum of the digits is divided by 9 would be $0 + 6$, which is 6. Are there other places in the check where work could have been shortened? We thus, in a way, throw away the nines. It was from this that the name "casting out the nines" came.

By just the same principle, in a numeration system to the base 7 one would cast out the sixes, to the base 12 cast out the elevens, etc.

7. Divisibility by 11

There is a test for divisibility by 11 which is not quite so simple as that for divisibility by 9 but is quite easy to apply. In fact, there are two tests. We shall start you on one and let you discover the other for yourself. Suppose we wish to test the number 17945 for divisibility by 11. Then we can write it as before

$$(1 \cdot 10^4) + (7 \cdot 10^3) + (9 \cdot 10^2) + (4 \cdot 10^1) + 5.$$

The remainders when 10^2 and 10^4 are divided by 11 are 1. But the remainders when 10 , 10^3 and 10^5 are divided by 11 are 10. Now 10 is equal to $11 - 1$. $10^3 = 10^2 (11 - 1)$, $10^5 = 10^4 (11 - 1)$. That is enough. Perhaps we have told you too much already. It is your turn to carry the ball.

Exercises 7a

1. Without considering 10 to be $11 - 1$, can you from the above devise a test for divisibility by 11?
2. Noticing that $10 = 11 - 1$ and so forth as above, can you devise another test for divisibility by 11?

We hope you were able to devise the two tests suggested in the previous exercises. For the first, we could group the digits and write the number 17945 as $(1 \times 10^4) + (79 \times 10^2) + 45$. Hence the remainder when the number 17945 is divided by 11 should be the same as the remainder when $1 + 79 + 45$ is divided by 11, that is, $1 + 2 + 1 = 4$. (2 is the remainder when 79 is divided by 11, etc.) This method would hold for any number.

The second method requires a little knowledge of negative numbers (either review them or, if you have not had them, omit this paragraph). We could consider -1 as the remainder when 10 is divided by 11, since $10 = 1(11) + (-1)$, where $q = 1$ and $r = -1$. Then the original number would have the same remainder as the remainder when $1 + [7(-1)^3] + 9 + [4(-1)] + 5$ is divided by 11, that is, when $5 - 4 + 9 - 4 + 1$ is divided by 11. This last sum is equal to 4, which was what we got the other way. By this test we start at the right and alternately add and subtract digits. This is simpler than the other one.

Exercises 7b

1. Test several numbers for divisibility by 11 using the two methods described above. Where the numbers are not divisible, find the remainders by the method given.
2. In a number system to the base 7, what number could we test for divisibility in the same way that we tested for 11 in the decimal system? Would both methods given above work for base 7 as well?
3. To test for divisibility by 11, we grouped the digits in pairs. What number or numbers could we test for divisibility by grouping the digits in triples? For example, we might consider the number 157892. We could form the sum of 157 and 892. For what numbers would the remainders be the same?
4. Answer the questions raised in Problem 3 in a numeral system to base 7, as well as in numeral system to base 12.
5. In the repeating decimal for $\frac{1}{9}$ in the decimal system, there is one digit in the repeating portion; in the repeating decimal for $\frac{1}{11}$ in the decimal system, there are two digits in the repeating portion. Is there any connection between these facts and the tests for divisibility for 9 and 11? What would be the connection between repeating decimals and the questions raised in Problem 3 above?
6. Could one have a check in which 11's were "cast out"?
7. Can you find a trick for 11 similar to that in Problem 1 above?

8. Divisibility by 7

There is not a very good test for divisibility by 7 in the decimal system. (In a numeration system to what base would there be a good test?) But it is worth looking into since we can see the connection between tests for divisibility and the repeating decimals. Consider the remainders when the powers of 10 are divided by 7. We put them in a little table:

n	1	2	3	4	5	6	7
Remainder when 10^n is divided by 7	3	2	6	4	5	1	3

If you compute the decimal equivalent for $\frac{1}{7}$, you will see that the remainders are exactly the numbers in the second line of the table in the order given. Why is this so? This means that if we wanted to find the remainder when 7984532 is divided by 7 we would write

$$(7 \times 10^6) + (9 \times 10^5) + (8 \times 10^4) + (4 \times 10^3) + (5 \times 10^2) + (3 \times 10) + 2$$

and replace the various powers of 10 by their remainders in the table to get

$$(7 \times 1) + (9 \times 5) + (8 \times 4) + (4 \times 6) + (5 \times 2) + (3 \times 3) + 2.$$

We would have to compute this, divide by 7, and find the remainder. That would be as much work as dividing by 7 in the first place. So this is not a practical test, but it does show the relationship between the repeating decimal and the test.

Notice that the sixth power of 10 has a remainder of 1 when it is divided by 7. If instead of 7 some other number is taken which has neither 2 nor 5 as a factor, 1 will be the remainder when some power of 10 is divided by that number. For instance, there is some power of 10 which has the remainder of 1 when it is divided by 23. This is very closely connected with the fact that the remainders must, from a certain point on, repeat. Another way of expressing this result is that one can form a number completely of 9's like 99999999, which is divisible by 23.

Exercises 8

Complete the following table. In doing this, notice that it is not necessary to divide 10^{10} by 17 to get the remainder when it is divided by 17. We can compute each entry from the one above like this: 10 is the remainder when 10 is divided by 17; this is the first entry. Then divide 10^2 , that is, 100 by 17, and see that the remainder is 15. But we do not need to divide 1000 by 17. We merely notice that 1000 is 100×10 and hence the remainder when 1000 is divided by 17 is the same as the remainder when 15×10 , or 150, is divided by 17. This remainder is 14. To find the remainder when 10^4 is divided by 17, notice that 10^4 is equal to $10^3 \times 10$ and hence the remainder when divided by 17 is the same as when 14×10 is divided by 17, that is, 4. The table then gives the remainders when the powers of 10 are divided by various numbers.

	3	7	9	11	13	17	19	21	37	101	41
1	1	1	1			1					
10^1	1	3	1			10					
10^2	1	2	1			15					
10^3	1	6	1			14					
10^4	1	4	1			4					
10^5	1	5	1			6					
10^6	1	1	1			9					
10^7	1		1			5					
10^8	1		1			16					
10^9	1		1			7					
10^{10}	1		1			2					
10^{11}	1		1			3					
10^{12}	1		1			13					
10^{13}	1		1			11					
10^{14}	1		1			8					
10^{15}	1		1			12					
10^{16}	1		1			1					

Find what relationships you can between the number of digits in the repeating decimals for $\frac{1}{3}$, $\frac{1}{7}$, $\frac{1}{9}$, $\frac{1}{11}$, $\frac{1}{13}$, etc., and the pattern of the remainders.

Why does the table show that there will be five digits in the repeating portion of the decimal for $\frac{1}{41}$? Will there be some other fraction $\frac{1}{q}$ which will have a repeating decimal with five digits in the repeating portion? How would you find a fraction $\frac{1}{q}$ which would have six digits in the repeating portion?

If you wish to explore these things further and find that you need help, you might begin to read some book on the theory of numbers. Also, there is quite a little material on tests for divisibility in "Mathematical Excursions" by Helen Abbott Merrill, Dover (1958).

9. Complete Factorization

Suppose we apply what we have learned about divisibility to a few examples:

Example 1 Find a complete factorization of 232. Since the given number has 2 as its last digit, it is even and has 2 as a factor. So, $232 = 2 \times 116$. Then 116 has 2 as a factor and we have $232 = 2^2 \times 58$. Then we have $232 = 2^3 \times 29$. We can see that 29 is a prime number by looking at our table of the Sieve of Eratosthenes or by trying the prime factors: 2, 3, 5, 7, 11, 13, 17, 19, 23 less than 29. Some of you may be able to see why it is necessary only to try 2, 3, and 5.

A tabular way of finding the complete factorization is the following:

232	116	58	29
2	2	2	29

where 2 is the first factor and 116 is the quotient; then 2 is a factor of 116 and 58 is the quotient, etc. A complete factorization, then, is on the second line.

Example 2 Find a complete factorization of 573. Here the last digit is odd and hence 2 is not a factor. But the sum of the digits is 15, which is divisible by 3. Hence, 3 is a factor of 573 and, dividing, we have $573 = 3 \times 191$. By our tests 2, 3, and 5 are not factors of 191. Trial shows that 7, 11, and 13 are not factors and, hence, 191 is a prime number. Why is it not necessary to try any primes larger than 13? Therefore, $573 = 3 \times 191$ is the complete factorization.

Example 3 Find a complete factorization of 539. Our tests show that none of 2, 3, and 5 are factors. If we try 7, we see that $539 = 7 \times 77 = 7^2 \times 11$, which is a complete factorization.

It is important to notice that the tests for divisibility depend on the number being written in the decimal system. For instance, the number 21 in the decimal system is written 30_{seven} in the system base seven. This number, 30_{seven} , is not even, in spite of the fact, that its last digit is zero. However, since 30_{seven} means $(3 \times \text{seven}) + 0$, the fact that the last digit is zero tells us that the number is divisible by seven.

If a number is written to the base seven it is very easy to tell whether or not it is divisible by seven; one merely looks to see if the last digit is zero.

The property of one number being a factor of another does not depend on the way it is written; for instance, seven is always a factor of twenty-one, no matter how it is written. But the tests for divisibility which we have given here depend on the system of numeration in which the number is written.

Exercises 9

1. Find the smallest prime factor of each of the following.
(a) 115 (b) 135 (c) 321 (d) 484 (e) 539 (f) 121
2. Find a complete factorization of each of the following.
(a) 39 (c) 81 (e) 180 (g) 378 (i) 576 (k) 1098
(b) 60 (d) 98 (f) 258 (h) 432 (j) 729 (l) 2324
3. Notice the list of multiples of 3. In going from 9 to 12, the units digit decreases from 9 to 2, and the tens digit increases from 0 to 1; hence, the sum of the digits decreases by $7 - 1$, or a net decrease of 6. Similarly, in going from 18 to 21, the first digit increases by 1, and the second decreases by 7. Is this always true when the tens digit increases by 1? What happens when one goes from 99 to 102, from 999 to 1002, etc? Can you see from this, that always for a multiple of 3, it is true that the sum of its digits is a multiple of 3?
4. Show that the test given for divisibility by 5 always works.
5. List the multiples of 9 and see if you can show from this the test for divisibility by 9.
6. Can you give a test for divisibility of 6 in the decimal system?
7. Can you give a test for divisibility by 15 in the decimal system?
8. Which of the following numbers are divisible by 2?
(a) 1111_{ten} (b) 1111_{seven} (c) 1111_{six} (d) 111_{three}
9. Suppose a number is written in the system to the base 7. Is it divisible by ten if its last digit is 0? Is it divisible by 3 if the sum of its digits is divisible by 3?

- #10. Answer the above questions for a system of numeration to the base twelve.
- #11. Find a test for divisibility by 6 in a system of numeration to the base seven.
- #12. Give a test for divisibility by 4 in the decimal system.

10. Greatest Common Factor

Consider the numbers 10 and 12. We see that both 10 and 12 are even numbers. They are both divisible by 2, or we may say that 10 and 12 are multiples of 2. Because 2 is a factor of 10 and is also a factor of 12, we say that 2 is a "common factor" of 10 and 12.

All whole numbers are multiples of 1. Thus, 1 is a common factor of the members of any set of whole numbers. Therefore, when we are looking for common factors, we generally look for numbers other than 1.

What factor other than 1 is common to both 12 and 15? Is 2 a common factor? Since 15 is odd, 2 is not a factor of 15. Therefore, it is impossible for 2 to be a common factor of 12 and 15. However, 12 and 15 are both multiples of 3. Hence, 3 is a common factor of 12 and 15.

Do the numbers 12 and 30 have any common factors? Writing the set of factors of 12 and the set of factors of 30 as shown at the right, we see that there are several common factors.

Set of factors of 12 is {1,2,3,4,6,12}

Set of factors of 30 is {1,2,3,5,6,10,15,30}

The numbers 1, 2, 3, and 6 are the common factors of 12 and 30.

Do the numbers 10 and 21 have any common factors? Writing the set of factors of 10 and the set of factors of 21 as shown at the right, we see that 10 and 21 do not have any common factors other than 1.

Set of factors of 10 is {1,2,5,10}

Set of factors of 21 is {1,3,7,21}

So, we see that for any set of whole numbers the numbers have the common factor 1. For some sets of whole numbers there is a common factor, other than 1, and, for some sets of whole numbers, there are several common factors other than 1.

Recognizing common factors is useful in many ways. You have already used the idea of common factors in changing fractions to lower terms. For example, in changing $\frac{10}{12}$ to $\frac{5}{6}$ you use the common factor, 2, of 10 and 12.

For $\frac{12}{30}$ we should see that 2 is a common factor of 12 and 30. The result is $\frac{6}{15}$. However, we see that for $\frac{6}{15}$ there is a common factor, 3, of 6 and 15. Thus, $\frac{6}{15}$ may be written as $\frac{2}{5}$.

Is it possible to change $\frac{12}{30}$ to $\frac{2}{5}$ using a single number instead of using 2 and 3 in turn? Some of you may have wondered why anyone would choose to change $\frac{12}{30}$ by using both 2 and 3 when it would be much quicker to use 6.

Is 6 a factor of both 12 and 30? Referring to the earlier listing of these factors, we see that 12 and 30 have the common factors 1, 2, 3, and 6. How does 6 differ from the other common factors? It is the largest of the common factors of 12 and 30. Such a factor is called the "greatest common factor".

Definition: The greatest common factor of two whole numbers is the largest whole number which is a factor of each of them.

Generally, the greatest common factor is more useful in mathematics than other common factors. Therefore, we are most interested in the greatest common factor.

Let's try another example. Suppose we wish to find the greatest common factor of 12 and 18. We could write the set of factors of each:

Set of factors of 12 is {1, 2, 3, 4, 6, 12}

Set of factors of 18 is {1, 2, 3, 6, 9, 18}

The set of common factors of 12 and 18 is {1, 2, 3, 6}. The largest member of the set is 6. Therefore, 6 is the greatest common factor of 12 and 18.

Similarly, suppose we wish to find the greatest common factor of 24 and 60. Writing the factors of each:

Set of factors of 24 is {1,2,3,4,6,8,12,24}

Set of factors of 60 is {1,2,3,4,5,6,10,12,15,20,30,60}

The set of common factors is {1,2,3,4,6,12}. The greatest of these factors is 12. Therefore, 12 is the greatest common factor of 24 and 60.

Exercises 10

1. Write the set of all factors for each of the following. List these carefully as you will use these sets in answering Problem 2 below.

(a) 6

(c) 12

(e) 16

(b) 8

(d) 15

(f) 21

2. Using your answers in Problem 1 above, write the set of common factors in each of the following cases.

(a) 6, 8

(c) 12, 15

(e) 12, 15, 21

(b) 8, 12

(d) 6, 8, 12

(f) 8, 12, 16

3. Write the set of all factors for each of the following.

(a) 19

(c) 36

(e) 45

(b) 28

(d) 40

(f) 72

4. Using your answers to Problems 1 and 3 above, write the set of common factors for each of the following.

(a) 19, 28

(c) 28, 40

(e) 40, 72

(b) 16, 36

(d) 36, 45

(f) 19, 36, 45

5. Using your answers to Problems 2 and 4 above, write the greatest common factor for each of the following cases.

(a) 8, 12, 16

(c) 28, 40

(e) 40, 72

(b) 16, 36

(d) 36, 45

(f) 8, 12, 16, 36

6. Find the greatest common factor in each of the following cases.

(a) 15, 25

(f) 15, 30, 36

(b) 18, 30

(g) 12, 24, 48

(c) 24, 36

(h) 40, 48, 72

(d) 25, 75

(i) 15, 30, 45

(e) 32, 48

(j) 20, 50, 100

7. (a) What is the greatest common factor of 6 and 6?
 (b) What is the greatest common factor of 29 and 29?
 (c) What is the greatest common factor of a and a where a is any counting number?
8. (a) What is the greatest common factor of 1 and 6?
 (b) What is the greatest common factor of 1 and 29?
 (c) What is the greatest common factor of 1 and a where a represents any whole number?
9. Let a and b represent any two different whole numbers where $a < b$.
 (a) Will a and b always have a common factor? If so, what is the factor?
 (b) Let c represent a common factor of a and b . Can $c = a$? If so, give an example.
 (c) Can $c = b$? If so, give an example.
10. Suppose 1 is the greatest common factor of three numbers.
 (a) Must one of the three numbers be a prime number? If not, write a set of three composite numbers whose greatest common factor is 1.
 (b) Can two of the numbers have a greatest common factor larger than 1? If so, give an example.
11. In finding the greatest common factor for a set of numbers it is sometimes troublesome to write out all the factors. Try to find a shorter way of obtaining the greatest common factor. Assume that you are to find the greatest common factor of 36 and 45.
 (a) Write a complete factorization of 36 and 45. (List all of the prime factors of 36 and of 45.)
 Example: $36 = 2 \cdot 2 \cdot 3 \cdot 3 \cdot 3 = 2^2 \cdot 3^3$
 $45 = ? \cdot ? \cdot ? = ? \cdot ?$
 (b) What is the greatest common factor of 36 and 45?
 (c) Compare the list of prime factors of 36 and 45 and the greatest common factor of 36 and 45. Can you see a shorter way of obtaining the greatest common factor?
12. (a) Write a complete factorization for 18 and for 90.
 (b) What is the greatest common factor of 18 and 90?

13. Factor completely each number in the following sets and find the greatest common factor for each set of numbers.

- | | |
|-----------------|--------------------|
| (a) {24,60} | * (f) {42,105,147} |
| (b) {36,90} | * (g) {165,234} |
| (c) {72,108} | * (h) {306,1173} |
| (d) {25,75,125} | * (i) {2040,2184} |
| (e) {24,60,84} | |

- *14. (a) What is the greatest common factor of 0 and 6?
 (b) What is the smallest common factor of 0 and 6?
 (c) What is the smallest common factor for any two whole numbers?

*15. You have learned about operations with whole numbers: addition, subtraction, multiplication, and division. In this section we studied the operation of finding the greatest common factor. This is sometimes abbreviated G.C.F. For this problem only, let us use the symbol " Δ " for the operation G.C.F. For any whole numbers, a and b and c,

$$a \Delta b = \text{G.C.F. for } a \text{ and } b$$

or

$$a \Delta c = \text{G.C.F. for } a \text{ and } c$$

Example:

$$12 \Delta 18 = 6$$

$$9 \Delta 15 = 3$$

- (a) Is the set of whole numbers closed under the operation Δ ?
 (b) Is the operation Δ commutative; that is, does $a \Delta b = b \Delta a$?
 (c) Is the operation Δ associative; that is, does
 $a \Delta (b \Delta c) = (a \Delta b) \Delta c$?

11. Remainders in Division

Another way to find the greatest common factor is to make use of a relationship among the parts of a division problem. To understand this method, let us review the division process.

The question, "What is the result of dividing 16 by 5?", may be stated, "How many 5's are contained in 16?"

We can find the answer by repeated subtraction, as shown at the right. By counting the number of times a 5 is subtracted, we obtain the answer, 3, with a remainder, 1. Does $16 = (5 + 5 + 5) + 1$?

$$\begin{array}{r} 16 \\ -5 \\ \hline 11 \\ -5 \\ \hline 6 \\ -5 \\ \hline 1 \end{array}$$

The usual way of finding the answer to this division problem is shown below:

$$\begin{array}{r} 3 \text{ Remainder } 1 \\ 5 \overline{)16} \\ \underline{15} \\ 1 \end{array}$$

To check the answer we use the following idea:

$$16 = (5 \times 3) + 1.$$

In the division problem above, the 16 is called the dividend, the 5 is the divisor, the 3 is the quotient, and the 1 is the remainder.

Let's try another example. Divide 253 by 25.

$$\begin{array}{r} 10 \text{ Remainder } 3 \\ 25 \overline{)253} \\ \underline{25} \\ 3 \end{array}$$

$$\text{Does } 253 = (25 \times 10) + 3?$$

In general, for any division problem:

$$\text{dividend} = (\text{divisor} \times \text{quotient}) + \text{remainder}$$

Using mathematical symbols, where

- "a" represents the dividend,
- "b" represents the divisor,
- "q" represents the quotient,
- "R" represents the remainder.

This division relation may be expressed as follows:

$$a = (b \cdot q) + R$$

Consider the following example in division:

$$\begin{array}{r} 24 \text{ Remainder } 23 \\ 25 \overline{)623} \\ \underline{50} \\ 123 \\ \underline{100} \\ 23 \end{array}$$

We can write this problem in the form

$$623 = (25 \times 24) + 23.$$

This follows the general form:

$$\text{dividend} = (\text{divisor} \times \text{quotient}) + \text{remainder}$$

or

$$a = (b \cdot q) + R$$

Exercises 11

1. Copy and complete the following table. Do this carefully as you will use the table in answering Problem 2.

	DIVIDEND = (DIVISOR · QUOTIENT) + REMAINDER			
EXAMPLE	9	4	2	1
a.	12	6	?	0
b.	14	3	?	?
c.	29	?	3	2
d.	37	5	?	?
e.	38	9	?	?
f.	41	13	?	?
g.	59	?	5	9
h.	?	11	6	0
i.	77	?	3	17
j.	81	?	?	0

2. Use the table in Problem 1 in answering parts a, b, and c.
- Compare the divisor and quotient in each part. Does one of these always have the greater value in a division problem?
 - Compare the quotient and dividend. Which one has the greater value if the dividend and divisor are both counting numbers?
 - Compare the divisor and the remainder. Which one always has the greater value in a division problem?
 - Can the dividend be zero? If so, give an example.
 - Can the divisor be zero? If so, give an example.
 - Can the quotient be zero? If so, give an example.
 - Can the remainder be zero? If so, give an example.

3. Using the table in Problem 1, answer the following questions.
- Can any whole number appear as a dividend? If not, give an example.
 - Can any whole number appear as a divisor? If not, give an example.
 - Can any whole number appear as a quotient? If not, give an example.
 - Must the remainder always be some whole number? Explain.
4. Copy and complete the following table for the division relation.

$$a = (b \cdot q) + R$$

	a	b	q	R
a.	15	?	7	?
b.	?	10	9	8
c.	50	12	?	?
d.	100	?	?	0
e.	283	17	?	?
f.	630	?	25	5

5. Using the table above answer the following.
- Can R be greater than b ? If so, give an example.
 - Can q be greater than b ? If so, give an example.
 - Can R be greater than the quotient, q ? If so, give an example.
 - Can any whole number be a possible value of b ? Explain.
 - Can any counting number be a possible value of b ? Explain.
 - Can any whole number be a possible value of a ? Explain.
6. Using the division relation, $a = (b \cdot q) + R$, where $R < b$, answer the following.
- If $b = 4$, write the set of all possible remainders.
 - If $b = 11$, describe the set of all possible remainders.
 - If all the possible remainders in a division problem are the whole numbers less than 25, what is b ?
 - If $b = K$, which one of the following represents the number of all possible remainders?
 (K) , $(K + 1)$, or $(K - 1)$

- * 7. By using the division relation we have a method for finding the greatest common factor of two numbers.

Example A: Find the greatest common factor of 12 and 8.

- (1) First, divide the larger number by the smaller:
12 divided by 8 = 1; Remainder 4
- (2) Second, divide the divisor, 8, by the remainder, 4:
8 divided by 4 = 2; Remainder 0
- (3) The 4 is the last divisor used which gives a remainder of 0. The greatest common factor of 8 and 12 is 4.

Example B: Find the greatest common factor of 35 and 56.

- (1) First, divide the larger number, 56, by the smaller number, 35.

$$\begin{array}{r} 1 \text{ Remainder } 21 \\ 35 \overline{)56} \\ \underline{35} \\ 21 \end{array}$$

- (2) Second, divide the divisor, 35, by the remainder, 21.

$$\begin{array}{r} 1 \text{ Remainder } 14 \\ 21 \overline{)35} \\ \underline{21} \\ 14 \end{array}$$

- (3) Next, continue dividing the last divisor by the last remainder until the remainder is 0.

$$\begin{array}{r} 1 \text{ Remainder } 7 \\ 14 \overline{)21} \\ \underline{14} \\ 7 \end{array} \qquad \begin{array}{r} 2 \text{ Remainder } 0 \\ 7 \overline{)14} \\ \underline{14} \\ 0 \end{array}$$

The last divisor used is the greatest common factor.

The 7 is the greatest common factor of 35 and 56.

Note that when 14 is divided by 7, the remainder is 0.

The 7 is the last divisor used.

Using the above method, find the greatest common factor for each of the following pairs of numbers.

- | | |
|----------------|---------------------|
| (a) 32 and 92 | * (d) 124 and 836 |
| (b) 81 and 192 | * (e) 336 and 812 |
| (c) 72 and 150 | * (f) 1207 and 1349 |

12. Least Common Multiple

You have already learned a great deal about multiples of numbers:

that all whole numbers are multiples of 1;

that even numbers $\{0, 2, 4, 6, \dots\}$ are multiples of 2;

that $\{0, 3, 6, 9, \dots\}$ are multiples of 3.

Similarly, we can list the multiples of any counting number.

The number 2 is an even number, and the number 3 is an odd number. Usually we do not think of such numbers as having much in common. Yet, if we look at the set of multiples of 2 and the set of multiples of 3, we see that they do have something in common. Some of the multiples of 2 are also multiples of 3. For example, 6 is a multiple of both 2 and 3. There are many such numbers divisible by both 2 and 3. The set of these numbers is written as follows:

$$\{6, 12, 18, 24, 30, \dots\}$$

Definition: Numbers which are multiples of more than one number are called common multiples of those numbers. "Common" means belonging to more than one. Thus, 6 and 12 are common multiples of 2 and 3.

Let's try another example. List the common multiples of 3 and 4. First, we list the multiples of each:

Set of multiples of 3: $\{0, 3, 6, 9, 12, 15, 18, 21, 24, \dots\}$

Set of multiples of 4: $\{0, 4, 8, 12, 16, 20, 24, \dots\}$

The numbers that these sets have in common are the common multiples of 3 and 4. This set is written as follows:

$$\{0, 12, 24, 36, 48, \dots\}$$

Common multiples are very useful in arithmetic. For example, let us add $\frac{1}{2} + \frac{1}{3}$. We write $\frac{1}{2}$ as $\frac{3}{6}$ and $\frac{1}{3}$ as $\frac{2}{6}$. Then $\frac{3}{6} + \frac{2}{6} = \frac{3+2}{6} = \frac{5}{6}$.

Here we use a common multiple of 2 and 3. In doing such problems, you may have called the 6 a "common denominator". It is a common multiple of the denominators of the given fractions.

Since 6, 12, 18, and so on, are multiples of 2 and 3, we can use any of these numbers in adding $\frac{1}{2} + \frac{1}{3}$. Notice that the number, 6, which we did use is the smallest of those possible. It is also the smallest of the common multiples of 2 and 3. The number, 6, is called the least common multiple of 2 and 3.

Definition: The least common multiple of a set of counting numbers is the smallest counting number which is a multiple of each member of the set of given numbers.

Suppose we wish to find the least common multiple of 12 and 18. First, we list the sets of multiples of each:

Set of Multiples of 12: {0,12,24,36,48,60,72,84,...}

Set of Multiples of 18: {0,18,36,54,72,...}

The set of common multiples of 12 and 18 is {0,36,72,108,...}. The smallest counting number in this set is 36. Therefore, 36 is the least common multiple of 12 and 18.

What is the least common multiple of 2, 3, and 4?

Set of Multiples of 2: {0,2,4,6,8,10,12,...}

Set of Multiples of 3: {0,3,6,9,12,15,...}

Set of Multiples of 4: {0,4,8,12,16,20,...}

The set of common multiples of 2, 3, and 4 is: {0,12,24,36,...}. What is the smallest counting number in this set? According to our definition, the least common multiple of 2, 3, and 4 is 12.

Exercises 12

1. Write the set of all multiples less than 100 for each of the following.
 - (a) 6
 - (b) 8
 - (c) 9
 - (d) 12
2. Using your answers in Problem 1, write the set of all common multiples less than 100 for each of the following.

(a) 6 and 8	(d) 8 and 9
(b) 6 and 9	(e) 8 and 12
(c) 6 and 12	(f) 9 and 12
3. Using your answers in Problem 2, write the least common multiple of the elements of each of the following sets.

(a) 6 and 8	(d) 8 and 9
(b) 6 and 9	(e) 8 and 12
(c) 6 and 12	(f) 9 and 12

4. Find the least common multiple of the elements of each of the following sets.
- | | |
|-------------|--------------|
| (a) {2,5} | (e) {2,5,6} |
| (b) {4,6} | (f) {4,5,6} |
| (c) {2,3,5} | (g) {2,6,7} |
| (d) {3,4,6} | (h) {8,9,12} |
5. Find the least common multiple of the elements of the following sets.
- | | |
|------------|-------------|
| (a) {2,3} | (g) {2,13} |
| (b) {3,5} | (h) {7,11} |
| (c) {3,7} | (i) {3,13} |
| (d) {5,7} | (j) {11,13} |
| (e) {2,11} | (k) {2,3,5} |
| (f) {5,11} | (l) {23,29} |
6. Refer to Problem 5 and answer the following questions.
- To which set do the numbers 2, 3, 5, 7, 11, 13, 23, and 29 belong -- the set of composite numbers or prime numbers?
 - From your answers in Problem 5, what appears to be an easy way to find the least common multiple in those cases?
7. Find the least common multiple for each of the following sets.
- | | |
|------------|----------------|
| (a) {4,6} | (f) {10,12} |
| (b) {4,8} | (g) {12,15} |
| (c) {4,10} | (h) {4,6,10} |
| (d) {6,9} | (i) {10,15,30} |
| (e) {8,10} | (j) {4,6,8} |
8. In Problem 7, to which set of numbers, composite or prime, do each of the numbers, 4, 6, 8, ..., in parts (a) through (j) belong?
9. Compare the questions and your answers in Problems 7 and 8. Then answer the following.
- If c and d are composite counting numbers, can c or d be the least common multiple? Write an example to explain your answer.
 - If c and d are composite counting numbers, must c or d be the least common multiple? Write an example illustrating your answer.

10. (a) What is the least common multiple of 6 and 6?
 (b) What is the least common multiple of 29 and 29?
 (c) What is the least common multiple of a and a where a is any counting number?
11. (a) What is the least common multiple of 1 and 6?
 (b) What is the least common multiple of 1 and 29?
 (c) What is the least common multiple of 1 and a where a represents any counting number?
12. (a) If a and b are different prime numbers, can a or b represent the least common multiple of a and b ?
 (b) If a and b are different prime numbers, how can we represent the least common multiple of a and b ?
 *(c) If a , b , and c are different prime numbers, what is the least common multiple of a , b , and c ?
13. Study the following examples. Try to discover a shorter way to determine the least common multiple.

Example A: To find the least common multiple of 4, 6, and 8:

- (1) First, write a complete factorization for each number.

$$4 = 2^2 \qquad 6 = 2 \cdot 3 \qquad 8 = 2^3$$

- (2) The least common multiple is $2^3 \cdot 3$ or 24.

- (3) Note that $2^2 \cdot 2 \cdot 3 \cdot 2^3 = 192$, which is a common multiple of 4, 6, and 8, but not the least.

Example B: To find the least common multiple of 12 and 18:

- (1) A complete factorization for each number:

$$12 = 2^2 \cdot 3 \qquad 18 = 2 \cdot 3^2$$

- (2) The least common multiple of 12 and 18 is $2^2 \cdot 3^2$ or 36.

- (3) Is $(2^2 \cdot 3 \cdot 2 \cdot 3^2)$ a common multiple of 12 and 18?

- (4) Is $(2^2 \cdot 3 \cdot 2 \cdot 3^2)$ the least common multiple of 12 and 18?

Now find the least common multiple of each set in the following parts.

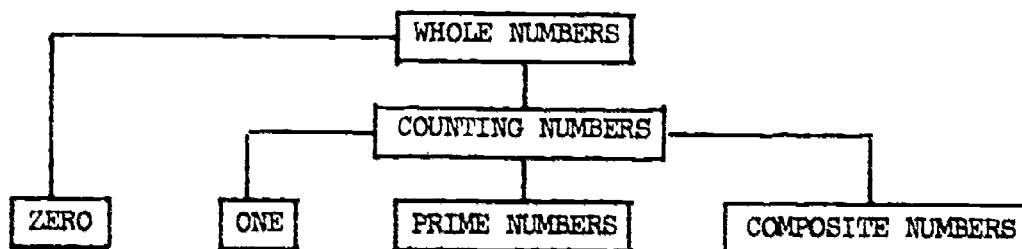
- (a) 12, 16
- (b) 14, 16
- (c) 9, 15
- (d) 10, 14
- (e) 16, 18
- (f) 4, 5, 6
- (g) 6, 8, 9

- (h) 8, 9, 10
- (i) 12, 20, 22
- (j) 9, 16, 20
- *(k) 250, 200
- *(l) 324, 144, 180
- *(m) 306, 1173

- *14. (a) Is there a greatest common multiple of 3 and 5? If so, write an example.
- (b) Is there a greatest common multiple of 4 and 6? If so, write an example.
- (c) Is there a greatest common multiple of any set of counting numbers?
- *15. (a) May we consider 0 as a multiple of zero? (Does $0 \times 0 = 0$?)
- (b) May we consider 0 as a multiple of six? (Does $6 \times 0 = 0$?)
- (c) May we consider 0 as a multiple of a , if a is any whole number?
- (d) Assume the least common multiple was defined as "the smallest whole number" instead of "the smallest counting number". What would be the least common multiple for any set of counting numbers?
- (e) Using the correct definition for least common multiple, is there a least common multiple for any counting number and 0?

13. Sub-sets of Whole Numbers

In this booklet you have studied whole numbers for the most part. Also, you have studied some important subsets of whole numbers. These subsets are shown in the sketch below:



Note that zero is a member of the set of whole numbers, but not a member of the set of counting numbers. The ONE, the PRIME NUMBERS, and the COMPOSITE NUMBERS are members of the set of COUNTING NUMBERS and also members of the set of WHOLE NUMBERS.

Every member of the set of counting numbers is a member of the set of whole numbers.

You learned that a PRIME number is any counting number other than 1 that is divisible only by itself and 1. The number 1 is not a prime number. We chose not to include 1 as a prime number because any number can be expressed as the product of primes in many different ways if we include 1 in the set of prime numbers.

A COMPOSITE number is a counting number, other than 1, that is not prime. Composite numbers have more than two factors.

The term "factor" was used instead of the words multiplicand and multiplier. The number, a , is a FACTOR of b if b is divisible by a . The set of factors of a number contains all counting numbers which are factors. A COMPLETE FACTORIZATION of a number represents the number as a product of prime numbers. For a prime number this is the number itself. For a composite number there are three or more factors. The UNIQUE FACTORIZATION PROPERTY of counting numbers refers to the fact that every composite number can be expressed as the product of primes in only one way, except for order.

A COMMON FACTOR of a set of whole numbers is a number that is a factor of each member of the set of numbers. The GREATEST COMMON FACTOR of a set of whole numbers is the largest counting number which is a factor of each member of the set of numbers. A common factor can never be greater than the largest member of the set.

The whole number, b , is a MULTIPLE of the whole number, a , if $a \cdot c = b$, where c is also a whole number. A COMMON MULTIPLE of a set of numbers is a multiple of each member of the set of numbers. The LEAST COMMON MULTIPLE is the smallest counting number which is a multiple of every member of the set of numbers. The least common multiple cannot be less than the largest member of the set of numbers.

Exercises 13

1. Find the greatest common factor of the numbers in each of the following sets of numbers.

(a) {2,3}

(e) {12,36}

(i) {39,51}

(b) {6,8}

(f) {15,21}

* (j) {74,146}

(c) {7,14}

(g) {23,43}

* (k) {45,72,252}

(d) {15,25}

(h) {66,78}

** (l) {44,92,124}

2. Find the least common multiple of the numbers in each of the sets of numbers in parts (a) through (1) in Problem 1.
3. (a) Find the product of the members of each set of numbers in Problem 1.
 (b) Find the product of the greatest common factor and the least common multiple for each set of numbers in Problem 1. (Refer to your answers for Problem 1 and Problem 2.)
 (c) How do your answers for (a) and (b) compare?
4. (a) Write the set of all composite numbers less than 31.
 (b) Write the set of all prime numbers less than 51.
5. Let a and b represent two counting numbers. Suppose that the greatest common factor of a and b is 1.
 (a) What is the least common multiple of a and b ? Give an example to explain your answer.
 (b) Would your answer for part (a) be true if you started with three counting numbers a , b , and c ? (Remember, the greatest common factor is 1.) Give an example to explain your answer.
6. (a) Can a prime number be even? Give an example to explain your answer.
 (b) Can a prime number be odd? Give an example to explain your answer.
 (c) How many prime numbers end with the digit 5?
 (d) With the exception of two prime numbers, all primes end with one of four digits. Write the two primes which are exceptions.
 (e) Write the other four digits which occur in the ones' place for all primes other than the exceptions you found in part (d).
7. Suppose the greatest common factor of two numbers is the same as their least common multiple. What must be true about the numbers? Give examples to explain your answer.
8. (a) What is the least common factor of 2867 and 6431?
 (b) What is the greatest common multiple of 2867 and 6431?
9. 112 tulip bulbs are to be planted in a garden. Describe all possible arrangements of the bulbs if they are to be planted in straight rows with an equal number of bulbs per row.

10. Two bells are set so that their time interval for striking is different. Assume that, at the beginning, both of the bells strike at the same time.
- (a) One bell strikes every three minutes and the second strikes every five minutes. If both bells strike together at 12:00 noon, when will they again strike together?
 - (b) One bell strikes every six minutes and the second bell every fifteen minutes. If both strike at 12:00 noon, when will they again strike together?
 - (c) Find the least common multiple of 3 and 5, and of 6 and 15. How do these answers compare with parts (a) and (b)?
11. (a) Can the greatest common factor of some whole numbers ever be the same number as the least common multiple of those whole numbers? If so, give an example.
- (b) Can the greatest common factor of some whole numbers ever be greater than the least common multiple of those numbers? If so, give an example.
- (c) Can the least common multiple for some whole numbers ever be less than the greatest common factor of those whole numbers? If so, give an example.
- *12. (a) Is it possible to have exactly four composite numbers between two consecutive primes? If so, give an example.
- (b) Is it possible to have exactly five consecutive composite numbers between two consecutive primes? If so, give an example.
- *13. Given the numbers 135, 222, 783, and 1065, without dividing, answer the following questions. Then check your answers by dividing.
- (a) Which numbers are divisible by 3?
 - (b) Which numbers are divisible by 6?
 - (c) Which numbers are divisible by 9?
 - (d) Which numbers are divisible by 5?
 - (e) Which numbers are divisible by 15?
 - (f) Which numbers are divisible by 4?
- *14. Why is it important to learn about prime numbers?
15. BRAINBUSTER. Ten tulip bulbs are to be planted so that there will be exactly five rows with four bulbs in each row. Draw a diagram of this arrangement.

16. BRAINBUSTER. Do you think there is a largest prime number? Can you find it or can you give a reason why you think there is no greatest one?
-

14. Robinson's Results

We are going to report to you on results published by Professor Raphael M. Robinson, of the University of California at Berkeley, in the October, 1958, issue of the "Proceedings of the American Mathematical Society". This will give you some idea of how research mathematicians are applying high-speed computers to solve problems about primes.

Robinson's note is based on calculations carried out during 1956 and 1957 on the SWAC (Standards Western Automatic Computer) at the University of California at Los Angeles.

To obtain an idea of the meaning of this work, let us think for a moment about the problem of finding out whether a given number, n , is a prime. According to the definition of a prime, we must find out whether n is divisible by some smaller number other than 1. The most obvious method is to divide n by the numbers, 2, 3, 4, ..., up to $n - 1$. If any of these numbers divide evenly into n , then n is not a prime. If none of these divisions come out evenly, then n is a prime. This method requires $n - 2$ divisions. If n is about 10^{100} , and if each division requires .001 of a second, then this would take about 10^{97} seconds. How many seconds are there in a year? About how many years would this take?

We could shorten the work very much if we think a little. If n is not a prime, then n can be expressed as a product of two smaller numbers:

$$n = a \cdot b.$$

If a is the smaller of these factors, then n is at least $a \cdot a = a^2$.

$$n \geq a^2.$$

Therefore, if n is not a prime, then it is divisible by some number, a , whose square is, at most, n . To test whether n is a prime, it is enough to divide n by the numbers, 2, 3, ..., up to the largest number whose square is no larger than n . If $n \leq 1,000,000$, then we do not have to try any divisors greater than 1,000, since $1,000^2 = 1,000,000$. Thus to see whether 999,997 is a prime, we only need to divide by 2, 3, ..., 999. By this method we only need 998 divisions instead of 999,995 divisions in the previous method.

If n is about 10^{100} , then this method requires only about 10^{50} divisions, for $10^{50} \cdot 10^{50} = 10^{100}$. If each division takes .001 of a second, how many years would it take by this method to test whether n is a prime?

If we wish to test really large numbers, we must look for better methods so that we can obtain the answers in a reasonable time. Therefore, mathematicians try to find special classes of numbers which have special properties which enable us to reduce the work even more.

For example, a great deal of work has been done on numbers which are one less than a power of 2. We may represent such numbers in the form

$$n = 2^m - 1.$$

If $m = 2$, then $n = 2^2 - 1 = 4 - 1 = 3$, which is a prime. If $m = 4$, then $n = 2^4 - 1 = 16 - 1 = 15$, which is not a prime. If m is not a prime, then n cannot be a prime. But m may be a prime without n being a prime.

Exercises 14

1. Make a table for $n = 2^m - 1$, up to $m = 20$.

m	1	2	3	4	5	6	7	8	9	10	11	12	13	14-20
n	1	3	7	15	31									

2. Test the statements:

- (a) If m is divisible by 2, then n is divisible by 3.
 - (b) If m is divisible by 3, then n is divisible by 7.
 - (c) If m is divisible by 5, then n is divisible by 31.
 - (d) What is the general law?
-

15. Proth's Theorem

Robinson reports on numbers which are one more than a small multiple of a power of 2, that is, numbers of the form

$$n = (k \cdot 2^m) + 1,$$

where k is a small odd number.

He and his group tested for primeness all numbers of this form with $k < 100$ and $m < 512$, as well as a few larger numbers. First they divided by all numbers less than 10,000; and for $k \leq 7$ they tried divisors up to 100,000. After eliminating all small factors in this way, they then applied a theorem stated by Proth in 1878. Let us see if we cannot get some idea of what Proth's theorem says and how it is used without trying to examine all of the details.

Proth's theorem gives a method of testing numbers of the form $n = (k \cdot 2^m) + 1$ for primeness, provided the counting number, k , is odd and less than 2^m . We can avoid much of the complication of the statement of Proth's theorem if we restrict ourselves to the case where k is not divisible by 3. Thus we may use

$$k = 1, 5, 7, 11, 13, 17, \dots$$

$$m = 1, 2, 3, 4, 5, 6, 7, \dots$$

and we are able to test the numbers $n = (k \cdot 2^m) + 1$ for primeness. For these numbers, n , Proth's theorem states that:

n is prime if, and only if, it is a factor of

$$\frac{n-1}{3^2} + 1.$$

Does this look mysterious to you? It is likely that it does, because you are not a mathematician. It would very probably look a bit mysterious even to a mathematician if he didn't happen to be familiar with the special techniques which are needed for a proof of this particular theorem. If you will accept, however, our word that it is a true theorem (and a great many very respectable mathematicians will testify to its being true) then it should not be hard to see what it says and how it is used.

In the first place, what does $3^{\frac{n-1}{2}} + 1$ mean? The expression $\frac{n-1}{2}$ is being used as an exponent. The number, n , we are using here is odd. (Why? What is the form of n ?) Thus $n - 1$ is even, so that $\frac{n-1}{2}$ is a counting number. Thus, $3^{\frac{n-1}{2}} + 1$ is just one more than 3 raised to a counting number power. To test n for primeness, we need only find this number and then divide it by n . If this division comes out even, then n is a prime; otherwise n is a composite.

What numbers can we test for primeness by this method? Let us list a few of them in a table and then apply the test to some of them. Fill in the blank spaces in the table below. Remember that Proth's theorem requires that $0 < k < 2^m$, and that we have restricted ourselves to numbers, k , which are not divisible by 3.

k	m	$n = (k \cdot 2^m) + 1$
1	1	3
1	2	5
1	3	9
5	3	
7	3	57
1	4	
5	4	81
7	4	113
11	4	
13	4	209
1	5	33

k	m	$n = (k \cdot 2^m) + 1$
5	5	161
7	5	225
11	5	
1		65
	6	321
	5	417
	5	545
		2,817
		17,409
17		2,177
	10	7,169
		10,241

Now let us see how the test works for a few of these numbers. To refresh our memories we restate it here:

If $n = (k \cdot 2^m) + 1$ where $0 < k < 2^m$ and k is not divisible by 3, then n is prime if, and only if, it is a factor of

$$3^{\frac{n-1}{2}} + 1.$$

Example 1: Let $k = 1$ and $m = 2$ so that $n = 5$. (Look it up in the table.) We are testing 5 for primeness. In this case, $\frac{n-1}{2}$ is $\frac{4}{2}$ or 2, so

$$3^{\frac{n-1}{2}} + 1 = 3^2 + 1 = 9 + 1 = 10.$$

Is n a factor of $3^{\frac{n-1}{2}} + 1$? Is 5 a factor of 10? Yes, it is, so the test tells us that 5 is a prime. Does this check with what you already know?

Example 2: Let $k = 1$ and $m = 3$ so that $n = 9$. (Look it up.) We divide

$$3^{\frac{n-1}{2}} + 1 = 3^4 + 1 = 81 + 1 = 82$$

by 9. The division does not come out even, so the test tells us that 9 is not a prime. Does this check with what you already know about 9?

Example 3: If $k = 1$ and $m = 6$, then what is n ? The table should tell you that $n = 65$. If it does not, work it out again. $\frac{n-1}{2}$ is 32, so

$$3^{\frac{n-1}{2}} + 1 = 3^{32} + 1 = 1,853,020,188,851,842.$$

We would have to divide this number by 65 to continue the test. It would not be worth the effort, however, since we can easily recognize that 65 has 5 as a factor, and is therefore not a prime.

Example 4: Let $k = 7$ and $m = 4$ so that $n = (k \cdot 2^m) + 1 = 113$.

In this case, the number $3^{\frac{n-1}{2}} + 1 = 3^{56} + 1$, is 9 times the square of $1,853,020,188,851,842 + 1$. If you are ambitious, you may calculate this number and divide it by $n = 113$. The division will come out even if you do your work correctly, so what do you conclude about 113?

Examples 3 and 4 should convince us of one thing. Proth's theorem is not well suited for testing large numbers for primeness by hand calculation. Large computers, however, are constructed expressly to make calculations of the order of the ones which discouraged us above. And they do them quickly! On the SWAC the time for the test was no more than $1\frac{1}{2}$ minutes as long as $m < 512$. For m about 1000 and $k = 3, 5$, or 7 the test took about

7 minutes. The number $n = (7 \cdot 2^{1000}) + 1$, is larger than 10^{300} . Compare 7 minutes with the time it would take the machine to test 10^{300} for primeness by trying all possible factors. Earlier in this section you got some idea of this time for numbers of the order of 10^{100} .

For $k = 1$, the test had previously been carried out for all $m < 8192$, and the only primes of this form which have been found are the cases:

$$m = 0, 1, 2, 4, 8, \text{ and } 16.$$

The largest new prime discovered by this work is the case $k = 5$, $m = 1947$:

$$n = (5 \cdot 2^{1947}) + 1.$$

If you wish to estimate this number, first notice that

$$10^3 = 1000 < 2^{10} = 1024.$$

Therefore, we have

$$2^{1947} > 2^{1940} = (2^{10})^{194} > (10^3)^{194} = 10^{582}.$$

Therefore, n has more than 582 digits. On the other hand, notice that

$$2^{13} = 8096 < 10^4.$$

Therefore, we have

$$\begin{aligned} n &< 1 + (8 \cdot 2^{1947}) = 1 + (2^3 \cdot 2^{1947}) = 1 + 2^{1950} \\ &= 1 + (2^{13})^{150} < 1 + (10^4)^{150} \\ &= 1 + 10^{600}. \end{aligned}$$

Consequently, n has no more than 600 digits.

Remember that by using the theorem of Proth, this prime was discovered by a single division taking a matter of minutes. By using either of the cruder methods discussed before, at least 10^{291} divisions would have been necessary. How long would this have taken at the rate of a thousand divisions per second?

This number is the fourth largest prime known at present. The larger ones are the numbers

$$n = 2^m - 1$$

with $m = 3217, 2281, \text{ and } 2203$. The latter two were reported by Robinson in the "Proceedings of the American Mathematical Society" in 1954. The largest one was reported early in 1958 by H. Riesel in Mathematical Tables and Aids to Computation (page 60).

Example 5: Estimate the number of digits in each of three primes.

Perhaps you would be interested in the general statement of Proth's theorem. For numbers $n = (k \cdot 2^m) + 1$ with k divisible by 3, the important

difference in the test for primeness is that the number, $3^{\frac{n-1}{2}} + 1$, must be replaced by a new number. The number to use is of the form

$$\frac{n-1}{a^2} + 1$$

where a is a counting number which may have to be chosen differently for different values of k and m . The condition which a must satisfy will be found in the statement of Proth's theorem.

Theorem: Let $0 < k < 2^m$ and $n = (k \cdot 2^m) + 1$. Suppose a is a counting number which has the property: no sum of a and a multiple of n is a perfect square. (Alternative: the sum of a and a multiple of n is never a perfect square.)

Then n is a prime if, and only if, it is a factor of

$$\frac{n-1}{a^2} + 1.$$

The condition which a must satisfy is rather a strange one. It would seem that it might be difficult to find a number which satisfies it in some cases. We could never find such a number by any number of trial operations, for the condition which a must satisfy involves a statement about all multiples of n . We may reject some choices of a on the basis of a single calculation, though. If $k = 3$, and $m = 2$ so that $n = 3 \cdot 2^2 + 1 = 13$, then would $a = 4$ do? No, because $117 + a = 117 + 4 = 121$ is a perfect square, and 117 is a multiple of $n = 13$. To find a number, a , which we can be sure will fit the condition for a given n , then, we will have to use reasoning. We will have to reason that, for a certain number, a , no matter how many multiples of n we try, adding a will never give a perfect square. Mathematicians know enough about numbers so that finding such a number is not a very difficult problem. As you may have guessed from the discussion above, it is possible to show that whenever k is not divisible by 3, the number $a = 3$ satisfies the condition of the theorem. Once we have found the right number, a , to go with n , we can avoid the many tedious calculations necessary to test a large number for primeness. Instead of dividing n by

all prime numbers whose squares are less than n , we need only perform one calculation. We simply try the division

$$\frac{n-1}{(a^2 + 1) \div n};$$

if it comes out even, n is a prime, if not, n is not a prime.